IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	
	)	**No. 18 CR 789**
v.	)	
	)	**Hon. Gary Feinerman**
DENY MITROVICH,	)	
	)	
Defendants.	)	

SURRESPONSE IN SUPPORT OF HIS MOTION TO COMPEL DISCOVERY

Now comes the defendant, Deny Mitrovich, by and through his undersigned attorney, and respectfully submits the following surresponse in support of his motion to compel discovery:

"[Supervisory Special Agent Brooke Donahue] does not know minute details of this technique[.]" Government's Surreply ("Gov. Sur."), Docket No. 62, Exhibit A, pg. 2. This is the information the government wants this Court to rely on in denying Mr. Mitrovich's Motion to Compel. They have provided no documentation or communication supporting their position that no malware infiltrated Mr. Mitrovich's computer when his browser was routed out of the Tor network and onto the open internet. Because this is simply impossible. In a case that turn on the "minute" details, it is simply improper for the government to downplay the importance of these details, particularly when the discovery in this case trends towards the United States government being far more involved than they are letting on in this recent, eleventh-hour interview of SSA Donahue.

For the sake of attempting brevity, the undersigned is attaching an FBI report from 2015 that outlined the investigation into The Love Zone ("TLZ") website and their involvement with both the foreign governments and the malware itself (*attached as Exhibit A*). There are, however, certain portions that it is important to highlight for this Court that both show a small window into the government's direct involvement of this investigation and the techniques used:

- "[I]n early 2014, the MCCU initiated Operation Downfall II to target these websites and users of these websites. Examples of these hidden services are "The Love Zone" (Exhibit A, pg. 1);
- "In mid-2014, the FBI, MCCU, obtained the ability to identify IP addresses associated with certain users of TorChat and certain hidden services. . .These hidden services include "The Love Zone (TLZ)" (Exhibit A, pgs. 1-2);
- "Pursuant to the above information, in late 2014, the Queensland Police Service (QPS) in Australia and the New Zealand Police and Department of Internal Affairs (DIA) seized control of both sites" (Exhibit A, pg. 2);
- "Reports of each of these users were then generated by the QPS/DIA and provided to the MCCU for further identification" (Exhibit A, pg. 2); and,
- "As part of the investigation, the QPS also provided periodic backup copies of the "TLZ" website to the MCCU for review. . . Upon receiving these copies, the MCCU entered the data into a previously established database a that allows for easy searching and generating of reports" (Exhibit A, pgs. 2-3).

The limited discovery in this case makes two things clear, that the government was working together with foreign law enforcement and that there is simply nothing to show or prove what was actually done to make Mr. Mitrovich's computer leave the Tor browser and go onto the open internet. The government's position that they were not involved in this investigation is simply disingenuous, particularly as it was not

SSA Donahue who was directly involved in the investigation of TLZ and "cyberguy", it was not SSA Donahue who authored the original FBI reports or the affidavit in support of the search warrant, and by their own admission, does not know how the software worked. The research and caselaw clearly shows there was malware used, and it does not matter if the IP address was seized from the computer, the issue is whether the used malware trespassed the computer. Considering this is merely a motion to compel, Mr. Mitrovich has surely met his limited burden of establishing prima facia evidence that his Fourth Amendment rights were violated.

I. Joint Venture and Applicability of the Fourth Amendment To Foreign Law Enforcement Conduct That Shocks The Judicial Conscience

The government's recent filing, and the accompanying interview SSA Donahue corroborates the government's involvement in the investigation and, in fact, shows that the government was much more involved with the investigation and search of Mitrovich's computer than previously indicated—only strengthening the necessity for disclosing the discovery so that Mitrovich can rightfully vindicate his constitutional rights. Evidence obtained in a search of an United States citizen by foreign authorities can be admissible even if the search did not comply with the laws of the United States, including the Fourth Amendment. *United States v. Strokes*, 726 F.3d 880, 890 (7th Cir. 2013). There are, however two exceptions to the rule, and they are both can applicable here. First, the Fourth Amendment applies if the United States agents participated in the investigation with foreign law enforcement, making the investigation "a joint operation between American and foreign authorities." *Id*. at

890-91. This exception is commonly referred to "as the Joint Venture Doctrine." *United States v. Ferguson*, 508 F.Supp.2d 1, *4 (D.D.C. Sep. 10, 2017). Second, it is "well-established" that the Fourth Amendment applies if "the conduct of the foreign police shocks the judicial conscience." *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). Even with the limited discovery already tendered, both apply here and would be further clarified if the government is compelled to turn over their communications, as previously requested.

a. Joint Venture Doctrine

The known facts already align with finding that there was a joint venture between the government and foreign law enforcement agencies. Federal agencies can enter joint ventures by providing assistance to foreign agencies in conduct surveillance. *United State v. Peterson*, 812 F.2d 486, 490 (9th Cir. 1987). In *Peterson*, the DEA passed a tip along to Philippine authorities about drugs being smuggled through its county. *Id.* at 488. The Philippine authorities then placed wiretaps on people suspected of being involved with the shipment. *Id.*at 488-89. The Philippine then provided the DEA with the intercepts. *Id.* The DEA would assist in translating and decoding some of the intercepts and also advised the Philippine authorities in their relevance. *Id.* at 490. The Ninth Circuit held that the district court "erred in concluding that the operation was not a joint venture. *Id.* The DEA had been substantially involved with the investigation. *Id.* The DEA even "termed their actions a 'joint investigation' in their own testimony" which supported finding the finding that there was a joint venture. *Id.*; *see also United States v. Barona*, 56 F.3d 1087 (9th

Cir. 1995) (there was no err in finding a joint venture between the DEA and Dutch authorities where the DEA requesting a wiretap on two defendants staying in the Copenhagen hotel, the intercepts were forwarded to the DEA, and the DEA provided a Spanish interpreter to Dutch authorities).

More recently, the Seventh Circuit found a joint venture between ICE agents and Thai authorities where ICE agents initiated the investigation into the defendant. *United States v. Stokes*, 726 F.3d 880, 891 (7th Cir. 2013). The Seventh Circuit agreed with the district court finding that there was joint venture between ICE and Thai authorities based on the ICE agent's substantial participation in the investigation and search of the defendant's home in Thailand. *Id.* The Thai authorities undertook surveillance of the defendant at the "behest" of ICE agents. *United States v. Stokes*, 710 F.Supp.3d 689, 697 (N.D. Ill. Dec. 11, 2009). The authorities then searched the defendant's home and the ICE authorities assisted in the search. *Id.* The Thai authorities initially seized the items but turned the seized items over to the ICE later that day. *Id.* The district court held that the agencies were in a joint venture while conducting the search even though the Thai authorities "directed the search" of the defendant's home. *Id.*

The government's filings, the 2015 FBI Report (Exhibit A), and SSA Donahue's recent interview indicates that United States authorities were acting in a joint venture with foreign law enforcements, which necessitates the need for further discovery. SSA Donahue, herself, seems to imply that the FBI's CEOU division initiated the investigation by determining the location of the TLZ hosting server in

the Netherlands. *See* Gov. Sur., Ex. A at 1. Once the government determined the location of the website, it passed along the information to Dutch authorities. *Id.* This was done for its own investigative purpose—so that the Dutch authorities could investigate further "and determine who was paying for the service site for TLZ." *Id.*; *see also* Exhibit A, pg. 2 ("Pursuant to the above information, in late 2014, the Queensland Police Service (QPS) in Australia and the New Zealand Police and Department of Internal Affairs (DIA) seized control of both sites"). This is similar, if not the same, as to what the DEA in *Peterson* did when it passed a tip along so that the Philippine authorities could set up a wiretap that would benefit the DEA in its own investigative purposes. Then, even though the Dutch authorities determined who was paying for hosting the server, the foreign authorities continued to give their findings over to the government even though they determined it was being paid for by an Australian individual. See Gov. Sur. at 8; *see also* Exhibit A, pgs. 2-3.

The government attempts claim that, at this point, the operation was only between the Dutch, Australian, and New Zealand authorities. *Id*. However, SSA Donahue confirms that the communications "with other governmental law enforcement agencies regarding this investigation was done through CEOU" itself. *See* Gov. Sur., Ex. A at 1; *see also* Exhibit A, pgs. 2-3.

The government and SSA Donahue try to distance the FBI's involvement in the investigation by stating that they did not advise QPS/DIA at all about using the technique nor did the QPS/DIA give notice to the FBI that it was going to use the technique. See Gov. Sur. at 8. The government, however, contradicts themselves

almost immediately by acknowledging that SSA Donahue and the QPS/DIA actually informed the FBI of their operation after they seized control of TLZ server and before they actually deployed their technique to identify users, essentially admitting they knew what was happening. Gov. Sur. at 8, n.5.

It is clear through what has already been disclosed by the government that there was a ongoing cooperative relationship between American and foreign law enforcement. If the FBI was not involved in the investigation at all after the individuals were located in Australia, then there would be no need for the foreign agencies to inform or contact the FBI in the middle of their investigation or notify them that they were deploying the technique.[1] This Court must scrutinize the government's position with what was originally reported in 2015 (Exhibit A). Much, if not all, is simply *non-sequitur* and contrary to their original reporting.

Further inquiry into how the government termed their investigation also supports finding a joint venture, just as it did in *Peterson*. SSA Donahue explains that child exploitation investigations "crosses borders, and requires the cooperation between the FBI and other countries." See Gov. Sur., Ex. A at 1. Here, the communications between agencies "regarding this investigation [were] done through CEOU." *Id*. The agencies continuously informed and shared information throughout the investigation.

[1] In her interview, SSA Donahue attempts to imply that the Australian authorities only notified foreign agencies after deploying the technique to avoid conflicts of ongoing undercover investigations. Gov. Sur., Ex. A at 2. However, if QPS/DIA used the technique because it did not know the identities of the users, then it is unclear how informing foreign agencies of their technique could affect ongoing investigations—they did not know who the users were so they could not know which investigations could be affected.

What is more, when reporters inquired about TLZ investigation, a FBI spokesperson, Christopher Allen, stated, "The FBI, led by its Legal Attaches in numerous countries around the world, seeks to foster strategic partnerships with foreign law enforcement, intelligence, and security services as well as with other US government agencies by sharing knowledge, experience, capabilities and by exploring joint operational opportunities."[2] To that end, the FBI itself admits that it considers its investigation into TLZ a joint operation. This establishes necessary "prima facia showing that the requested items are material to [Mitrovich's] defense." *United States v. Thompson*, 944 F.2d 1331, 1342 (7th Cir. 1991). The government must disclose the requested material show that Mitrovich can formulate his defense. *See United States v. Soto-Zuniga*, 837 F.3d 992, 1003 (9th Cir. 2016).

b. Conduct that Shocks the Conscience

Courts have "inherent supervisory powers over the administration of federal justice" and must apply the Fourth Amendment to evidence seized by foreign authorities when the foreign authorities conduct is so egregious that it "shocks the judicial conscience." *United States v. Emmanuel*, 565 F.3d 1324, 1330 (11th Cir. 2009). The way foreign authorities administered and control TLZ server during this operation, at the very least with the government knowledge if now more, is extremely egregious conduct. The TLZ sting operated differently than the FBI did in the Playpen operation in a much more outrageous and shocking matter, and it was done

[2] *See* Joseph Cox, *Australian Authorities Hacked Computer in the US*, Motherboard, (Aug. 15, 2016) https://www.vice.com/en_us/article/mg79nb/australian-authorities-hacked-computers-in-the-us

so for a significantly longer period of time. They also actually perpetuated and distributed child pornography.

Courts have long-criticized egregious law enforcement conduct, particularly when their actions affect third parties who are not who targets of the investigation. *See United States v. Archer*, 486 F.2d 670, 676-77 (2nd Cir. 1973) ("Governmental 'investigation' involving participation in activities that result in injury to the rights of its citizens is a course that courts should be extremely reluctant to sanction); *see also United States v. Thoma*, 726 F.2d 1191, 1199 (7th Cir. 1984) ([W]e will closely examine those cases in which the Government misconduct injures third parties in some way.").

The TLZ investigation inflicted an unprecedent amount of harm unto third parties by administering the site and using real video clips of child pornography in their technique to identify users. And their harm was inflicted upon a vulnerable class—abused and violated children. The Supreme Court has stated that anyone who distributes child pornography is culpable for the harm it inflicts upon children. *See Paroline v. United States*, 572 U.S. 1324, 457 (11th Cir. 2009) ("The unlawful conduct of everyone who reproduces, distributes, or possesses the images of the victim's abuse…plays a part in sustaining and aggravating this tragedy."); *see also New York v. Ferber*, 458 U.S. 747, 759 (1982) (finding that distributing child pornography is related to child abuse in at least two ways: 1) it creates a permanent record of the child's participation and the harm is exacerbated by its circulation; and 2) "the distribution network for child pornography must be closed if the production of

material which requires the sexual exploitation of children is to be effectively controlled.").

Federal courts have firmly criticized law enforcement misconduct while investigating child pornography offenses that was much less outrageous than the conduct here. Before the dark web, one way that law enforcement investigated child pornography offenses was to respond to newsletter ads which solicited child pornography. *See United States v. Chin*, 934 F.2d 393, 395-96 (2nd Cir. 1991). In *Chin*, the Second Circuit scolded the investigator for the harm he caused by encouraging the defendant to take elicit photos of children. *Id*. at 399. This one factor distinguished the investigator's conduct from "the usual undercover operation" and raised "very serious concerns with respect to the rights of third parties—namely, the rights of the children Congress sought to protect in enacting the prohibition on child pornography." *Id*. The court found that unlike normal sting operations, "the government agent in this case encouraged Chin to go out and commit a *real* crime, with *real* victims, just so Chin could be later arrested and prosecuted." *Id*.

Each time child pornography is purchased, it increases the demand and "serves to further the sexual exploitation of minors." *Id*. The less offensive Playpen watering hole operation was also heavily criticized by courts. *See United States v. Anzalone*, 221 F.Supp.3d 189, 194-95 (D. Mass. Sep. 28, 2016). In *Analone*, the court found that "[i]t is troubling that an agent stated the Producer's Pen [a section of Playpen's site] would be returning in the future because that section might have encouraged member to produce and share new child pornography." *Id*. Unlike in this matter, the conduct

was only allowed because the upload feature was never brought back online, the FBI did not advertise the child pornography to attract new users, and the FBI did not take any action to enhance the site's functionality. *Id*. at 195. Here, the purpose was to keep it up and continuously attract new users – at least thirty-three of them to be sure. *See* Exhibit A, pg.3.

The way QPS/DIA administered the site was much more egregious than any other child pornography investigation or water hole sting done by law enforcement in the United States. And it was all done with the government's knowledge. *See* Gov. Sur., n. 5 ("The FBI was informed of the Australian operation after they had already taken control of TLZ *and were prepared to utilize* their technique to identify individual users." (emphasis provided)). The hyperlink itself that QPS/DIA sent to users to deploy their identification technique, contained a "preview" of actual child pornography. *See* Dkt. 53 at 2. Then when users clicked the link, the QPS/DIA used real child pornography while deploying their technique. *Id*. This means that the QPS/DIA was actually distributing real child pornography that harmed real child victims. All with the knowledge and coordination of the government.

Further, news articles indicate that the QPS/DIA administered and controlled TLZ for six months.[3] During this time, users were still required to upload new material and TLZ had tens of thousands of users. *Id*. This means that during the TLZ investigation, potentially tens of thousands—if not hundreds of thousands— of new

[3] Michael Safi, *The Takeover: How Police Ended Up Running A Pedophile Site*, The Guardian, (Jul. 12, 2016) https://www.theguardian.com/society/2016/jul/13/shining-a-light-on-the-dark-web-how-the-police-ended-up-running-a-paedophile-site

child pornography were being uploaded and distributed under the control of QPS/DIA and, at the very least, the government's knowledge. It is shocking that QPS/DIA and the government allowed so many innocent third-party children to be abused so that it could arrest more people than it had already caught as opposed to shutting down the website.

The operation was much more massive in scope than the already criticized Playpen watering hole stings, during which the FBI had only controlled the server for less than two weeks. *United States v. Knowles*, 207 F.Supp.3d 585, 594 (D.S.C. Sep. 14, 2016). Also, unlike here, FBI did not have the upload feature functioning while it controlled the Playpen server. *Anzalone*, 221 F.Supp.3d at 195. From the little-known facts disclosed at this point, the investigation into TLZ harmed third parties in a way that no other child pornography investigation has been done before. The outrageous conduct of QPS/DIA is the exact type of conduct which makes the exception to the general rule on evidence obtained by foreign authorities applicable. And the government knew about all of this and participated along the entire way.

II. Use of Malware is A Search and, Despite the Government's Assertions, Malware Was Used

For there to be a search, the government does not have to collect information from the infected computer, just invade it. The use of malware to force a person's home computer to act in a certain way is a search that implicates the Fourth Amendment and Circuit Courts that have addressed the Playpen cases have held so. *See United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 213, n.7 (3rd Cir. 2018); *United States v. Henderson*, 906 F.3d

1109, 1113 n.4 (9th Cir. 2018); *United States v. Workman*, 863 F,3d 1313 (10th Cir. 2017). In *Horton*, the Eighth Circuit distinguished the use of NIT from the cases where IP addresses are voluntarily provided to third parties. *Horton*, 863 F.3d at 1047. In the Playpen cases, "the FBI sent computer code to the defendants' respective computers that searched those computers for specific information and sent that information back to law enforcement. Even if a defendant has no reasonable expectation of privacy in his IP address, he has a reasonable expectation of privacy in the contents of his personal computer." *Id. citing United States v. Turner*, 839 F.3d 429, 434 (5th Cir. 2016) (stating "a privacy interest exists in the electronic contents of computers and cell phones.").

Other Circuits addressing whether a search occurred in the Playpen operation have reached the same conclusion as the *Horton* court. [4] In *Werdene*, the Third Circuit held that the district court erred when it found the investigative technique did not engage in a search. *Werdene*, 883 F.3d at 213, n.7. In fact, the government even agreed that the technique engaged in a search. *Id.* "The NIT obtained the IP address and other identifying information from Werdene's home computer and not from a third party, and Werdene had a reasonable expectation of privacy in his home computer." *Id. citing United States v. Lifshitz*, 369 F.3d 173, 190 (2nd Cir. 2004) ("Individuals generally have a reasonable expectation of privacy in their home computers"); *see also Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have

[4] The Seventh Circuit addressed three Playpen cases in a consolidated appeal but expressly did not address whether the NIT engages in a search. *See United States v. Kienast*, 907 F.3d 522, 527 (7th Cir. 2018) ("We need not decide, however, whether the searches violated the Fourth Amendment.").

a reasonable expectation of privacy in their home and in their belongings—including computers—inside the home."). The "deployment" of the investigative technique "therefore constituted a 'search' under the Fourth Amendment." *Id*. *See also United States v. Henderson*, 906 F.3d 1109, 1113 n.4 (9th Cir. 2018) ("The government concedes that a 'search' occurred when the NIT was deployed to users' computers and returned their identifying information. As two of our sister circuits have before us, we agree." *See, Weredene*, 883 F.3d at 213, n.7; *see also, Horton*, 863 F.3d at 1047).

The reasoning of the Circuit courts aligns with the Supreme Courts holdings in *Riley v. California*, 573 U.S. 373 (2014). The *Riley* Court rejected the argument that law enforcement did not need a search warrant to look through the phone's call log because a person does not have a reasonable expectation of privacy in that information which is voluntarily disclosed to third parties and obtainable by a pen register order. *Id.* at 400. The *Riley* court unanimously dismissed this argument, holding that there was "no dispute" that the officer engaged in a Fourth Amendment search. *Id.* It was irrelevant that person may not have an expectation of privacy in some of the contents of the phone because a person has an expectation in the phone more broadly. Phones contain "a digital record of nearly every aspect" of a person's life and a person has a reasonable expectation of privacy in the device. *Id*. at 395-96.[5] Moreover, even the call logs might contain more than just phone number voluntarily

[5] The *Riley* Court even called phones "minicomputers" which implies that a person would have a greater expectation of privacy in a computer and its contents. *Id.* at 394.

disclosed when a call is placed but may include "identifying information" that an individual might add. *Id*. at 400.

Despite SSA Donahue's unfounded and conclusory assertions, the hyperlink utilized in the TLZ sting operation was much more nefarious than a simply hyperlink to a video and contained some sort of malware. Reporters covering the investigation into TLZ have called it a government hack.[6] Christopher Soghoian, the former Principal Technologist for the ACLU and current Senior Advisor for Privacy and Cybersecurity for United States Senator Ron Wyden, specifically commented on the technique for identifying TLZ's users and stating, "[i]f they get your IP address from the Tor Browser, then it is law enforcement hacking."[7] SSA Donahue even admits that the link routed Mitrovich's internet traffic from the Tor Network to the open internet, meaning it forced his computer to send information in a way that it was not configured to do so in the Tor Browser.

While SSA Donahue purports that the link advised Mirovich it was taking him outside of Tor network, the government's court filings and the previously disclosed discovery contradict SSA Donahue's assertions. For example, in the government's Response to Defendant's Motion to Compel, it stated that when the link was clicked on "the member was advised that the user was attempting to open a video file from an external website." *See* Dkt. 53 at 2*; see also* Exhibit A, pg. 2 ("When users clicked

[6] *See* Joseph Cox, *Australian Authorities Hacked Computer in the US*, Motherboard, (Aug. 15, 2016) https://www.vice.com/en_us/article/mg79nb/australian-authorities-hacked-computers-in-the-us (stating that TLZ investigation "highlights how law enforcement around the world are increasingly pursuing targets overseas using hacking tools, raising legal questions around agencies' reach.").

[7] *Id*.

the hyperlink, they were advised they were attempting to access a video file from an external website").

When operating the Tor Browser, a link to an external website would still open in the Tor Browser.[8] An external site means a site different that the one Mitrovich was currently viewing—it does not mean that the site will funnel his traffic through a completely different internet protocol. Advising that the link is from an "external site" is substantially and significantly different than advising that the link "would be taking them outside of Tor." *See* Gov. Sur., Ex. A at 2.

This is precisely why the requested discovery is necessary for Mitrovich to prepare a meaningful Fourth Amendment suppression argument. The malware or technique that hyperlink utilized is precisely at the heart of the critical issues in Mitrovich's case. The government has continuously given inconsistent information on how the link operated, at times saying the link advised of an "external site" and then

[8] *See* FAQ: What Protections Does Tor Provide?, The Tor Project *available at* https://2019.www.torproject.org/docs/faq.html.en#WhatProtectionsDoesTorProvide ("Generally speaking, Tor aims to solve three privacy problems: First, Tor prevents websites and other services from learning your location, which they can use to build databases about your habits and interest. With Tor, your Internet connections don't give you away by default – now you can have the ability to choose, for each connection, how much information to reveal. Second, Tor prevents people from watching your traffic locally (such as your ISP or someone with access to your home wifi or router) from learning what information you're fetching and where you're fetching it from. It also stops them from deciding what you're allowed to learn and publish – if you can get to any part of the Tor network, you can reach any site on the Internet. Third, Tor routes your connection through more than one Tor relay so no single rely can learn what you're up to. Because these relays are run by different individuals or organizations, distributing trust provides more security than the old one hop proxy server."); *see also* FAQ: So I'm Totally Anonymous If I Use Tor?, The Tor Project *available at* https://2019.www.torproject.org/docs/faq.html.en#AmITotallyAnonymous ("First, Tor protects the network communications. It separates where you are from where you are going on the Internet. What content and data you transmit over Tor is controlled by you. If you login to Google or Facebook via Tor, the local ISP or network provider doesn't know you are visiting Google or Facebook. Google and Facebook don't know where you are in the world. However, since you have logged into their sites [using your personal login information], they know who you are.")

stating that it advised users that it would take them completely outside the Tor Network.

To that end, it is simply implausible that the link actually advised users that it would take them outside of the Tor Network. The whole purpose of using Tor to access elicit sites is to keep their online presence anonymous—it goes against all logic for a user of such an elicit site would voluntarily click on a link that expressly stated it was taking them off the Tor Network. Furthermore, SSA Donahue admits that she does not know the "minute details of the technique." *See* Gov. Sur., Ex. A at 2. These inconsistent positions further highlight the necessity of disclosing the details of the technique—the government itself has not even given a consistent position on how the malware or technique operated.

The way in which the malware, or hyperlink, actually operated is the central issue for Mitrovich's defense. *See United States v. Soto-Zuniga*, 837 F.3d 992, 1001-02 (9th Cir. 2016) (reversing the defendant's conviction after the district court erroneously denied a motion to compel discovery as the discovery went to "an issue that [was] central to his defense, because it could spell the difference in a suppression motion of the key physical evidence against him."); *see also United States v. Budziak*, 697 F.3d 1105, 1112-13 (9th Cir. 2012) ("In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless.").

Conclusion

For these reasons, and all of the reasons stated in defendant Deny Mitrovich's Motion to Compel Discovery and the subsequent reply, he respectfully asks this Honorable Court to grant his Motion to Compel Evidence and enter an order directing the government to turn over all requested discovery so that he can properly and sufficiently litigating a Fourth Amendment based motion to suppress.

Respectfully submitted,

/s Vadim A. Glozman
Attorney For The Defendant

Vadim A. Glozman
VADIM A. GLOZMAN LTD.
Attorney at Law
53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015

CERTIFICATE OF SERVICE

I, Vadim A. Glozman, an attorney for Defendant Deny Mitrovich, hereby certify that on this, the 20th day of March, 2020, I filed the above-described document on the CM-ECF system of the United States District Court for the Northern District of Illinois, which constitutes service of the same.

Respectfully submitted,

/s/ Vadim A. Glozman

Vadim A. Glozman
VADIM A. GLOZMAN LTD.
53 W. Jackson Blvd., Suite 1410
Chicago, IL 60604
(312) 726-9015